



**Privacy:
Where the Rubber Hits the Road**



Cindy Allard
Defense Privacy, Civil Liberties, and Transparency Division
Department Of Defense

Ramona Branch Oliver
Department of Labor


Centralized vs. Decentralized Programs



- **Centralized**
 - One Privacy Office handles all privacy needs of agency
- **Decentralized**
 - Each major agency component has Privacy Office
 - Work up through a Department-Level Office

- **Know which you're working with**

Considerations



- **Determine your area of responsibility**
 - Organizationally
 - Personnel (what are the numbers)
- **Priorities**
 - Look to authorities and guidance
 - Staffing
 - Professional development (yours)
 - PBWA (Privacy By Walking Around)
 - Communication with organizational POCs

Authorities and Guidance

- Federal Records Act
- Paperwork Reduction Act
- Privacy Act of 1974
- E-Government Act of 2002 (OMB Memo M-03-22)
- E.O. 13402, Strengthening Federal Efforts to Protect Against Identity Theft
 - OMB Memo M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
 - OMB Memo M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements

Create a Positive and Collaborative Culture

- Collaborative Nature of Overall Team
- Involvement in Various Program Areas
- Leadership Support

Administrative Compliance

Records Management

Program Manager

Privacy Impact Assessment


Collections (OMB/Internal)

Forms

Systems Of Records Notice

Build a Cohesive Team

- **Goals**
 - Compliance with Laws
 - Model Program(s)
- **Reach Out to Compliance Counterparts**
 - Compliance Programs
 - Complementary
- **Awareness of Compliance Needs – Not Mastery**
 - Integration, Communication, Awareness



It's About Balance


- **Balance**
 - Annual and specialized training
 - Breach reporting
 - Systems of Records Notices (new and continuous monitoring)
 - Privacy Act Statements (forms, websites and other collections)
 - Privacy Impact Assessments
 - SSN Reduction and Fraud Prevention
 - Survey Reviews
- **Work with your IT and CIO counterparts**

Risk

- **What are the vulnerabilities?**
 - E-Gov Act
 - FOIA
 - Privacy Act
 - IT system inventory
- **What do you know you don't know?**

Continuous Risk Management

- Very similar to compliance
- Failure to continuously review is a risk



Managing Privacy Risk

The foundation of any program should be the fair information practices:

- Minimize the personal information collected
- Give constructive notice before collecting it
- Maintain the best quality information
- Offer access and redress within the law
- Protect the information

Managing Security Risk

A great security program is no substitute for an effective privacy program.

- A system can be air tight and locked down – effectively operating at “zero” security risk
- But it may have already violated fair information practices about minimization, notice, access, and redress, not to mention Federal privacy laws
- “Protect” alone is not enough

Privacy and Security Risk

<p>Examples of privacy risk:</p> <ul style="list-style-type: none">• Over-collection• Unauthorized browsing• Function creep• Curiosity browsing• Poor data fidelity	<p>Examples of security risk:</p> <ul style="list-style-type: none">• Internet intrusions• Analog threats• Acts of God• Lax patch management
--	--

Education and Training

- Several types of training, audiences
- Initial and annual
- IT security need documentation, breach training
- Every employee needs handling training
- Specific training based on your agency
 - Intelligence
 - Law Enforcement
 - Information Sharing Environment (ISE)

Helpful Considerations

- Understand your legal and regulatory requirements
- Ask open-ended questions
- Embrace learning as an occupational necessity
- Frequent assessment is critical to success
- Seek feedback and be open to change
- Network (other privacy folks, program managers, etc.)
- Review policies-are they appropriate or is it just what has always been done?
- Know your priorities but be flexible
- Do not assume someone else is doing it
- Don't expect to resolve things immediately
- Don't get comfortable
- The buck stops with you

What Does Success Look Like?

- Define value
- Keep boss out of the Washington Post (it only takes one negative to prove a positive)
- Ensure operational components can complete their mission within the bounds of the law
- Metrics (Counting)
 - How many PASs, PIAs, SORNs?
 - How many policies issued?
 - How many PII incidents resolved?
 - How many people trained?
- Know that sometimes success is looks bad

Recap

- Where you fit
- How to identify and approach priorities
- Authorities
- Collaboration and teamwork
- Finding balance
- Risk
- Education and training
- Things to keep in mind
- Thoughts on success

References

- Locate authorities and implementing guidance
 - 5 U.S.C. 552(a)
 - OMB (<https://www.whitehouse.gov/omb>)
 - Agency implementation